Search Results

Search Results for: **[tamper AND (proof OR resistant) AND (chip or IC or circuit) AND processor]**
Found **59** of **121,820 searched.**

Search within Results

1 Processor microarchitecture II: AEGIS: architecture for tamper-evident and tamper-resistant processing 93%
G. Edward Suh , Dwaine Clarke , Blaise Gassend , Marten van Dijk , Srinivas Devadas
Proceedings of the 17th annual international conference on Supercomputing June 2003
We describe the architecture for a single-chip aegis processor which can be used to build computing systems secure against both physical and software attacks. Our architecture assumes that all components external to the processor, such as memory, are untrusted. We show two different implementations. In the first case, the core functionality of the operating system is trusted and implemented in a security kernel. We also describe a variant implementation assuming an untrusted operating s ...

2 Communication complexity of secure computation (extended abstract) 83%
Matthew Franklin , Moti Yung
Proceedings of the twenty-fourth annual ACM symposium on Theory of computing July 1992
A secret-ballot vote for a single proposition is an example of a secure distributed computation. The goal is for m participants to jointly compute the output of some n-ary function (in this case, the sum of the votes), while protecting their individual inputs against some form of misbehavior. In this paper, we initiate the investigation of the communication complexity of unconditionally secure multi-party computation, and its relation with variou ...

3 Authentication and authorization: Silicon physical random functions 83%
Blaise Gassend , Dwaine Clarke , Marten van Dijk , Srinivas Devadas
Proceedings of the 9th ACM conference on Computer and communications security November 2002
We introduce the notion of a Physical Random Function (PUF). We argue that a complex integrated circuit can be viewed as a silicon PUF and describe a technique to identify and authenticate individual integrated circuits (ICs).We describe several possible circuit realizations of different PUFs. These circuits have been implemented in commodity Field Programmable Gate Arrays (FPGAs). We present experiments which indicate that reliable authentication of individual FPGAs can be performed even in the ...

4 Stimulating cooperation in self-organizing mobile ad hoc networks 82%
Levente Buttyán , Jean-Pierre Hubaux
Mobile Networks and Applications October 2003
Volume 8 Issue 5
In military and rescue applications of mobile ad hoc networks, all the nodes belong to the same authority; therefore, they are motivated to cooperate in order to support the basic functions of the network. In this paper, we consider the case when each node is its own authority and tries to maximize the benefits it gets from the network. More precisely, we assume that the nodes are not willing to forward packets for the benefit of other nodes. This problem may arise in civilian applications of mo ...

5 Computer security: Implementation of fast RSA key generation on smart cards 82%
Chenghuai Lu , Andre L. M. dos Santos , Francisco R. Pimentel
Proceedings of the 2002 ACM symposium on Applied computing March 2002
Although smart cards are becoming used in an increasing number of applications, there is small literature of the implementation issues for smart cards. This paper describes the issues and considerations that need to be

taken into account when implementing the key generation step of a cryptographic algorithm widely used nowadays, RSA.Smart cards are used in many applications that require a tamper resistant area. Therefore, smart cards that use cryptography have to provide encryption, decryption, ...

6 Software engineering for security: a roadmap 82%
Premkumar T. Devanbu , Stuart Stubblebine
Proceedings of the conference on The future of Software engineering May 2000

7 Protocol failure in the escrowed encryption standard 82%
Matt Blaze
Proceedings of the 2nd ACM Conference on Computer and communications security November 1994
The Escrowed Encryption Standard (EES) defines a US Government family of cryptographic processors, popularly known as "Clipper" chips, intended to protect unclassified government and private-sector communications and data. A basic feature of key setup between pairs of EES processors involves the exchange of a "Law Enforcement Access Field" (LEAF) that contains an encrypted copy of the current session key. The LEAF is intended to facilitate government access to the cl ...

8 Efficient computation on oblivious RAMs 82%
R. Ostrovsky
Proceedings of the twenty-second annual ACM symposium on Theory of computing April 1990

9 Government, industry, and academia: Teaming to design high confidence information security applications 80%
W. B. Martin , P. D. White , W. M. Vanfleet
Proceedings of the third workshop on Formal methods in software practice August 2000
A trusted computing base requires true separation of processes. Modern approaches relegate separation to a component of the operating system called the kernel. Although the kernel represents only a small portion of the code of the entire operating system, it is among the most intensively used portions. With separation as the focus, this paper will describe a kernel that provides strict separation between processes, allowing for the remainder of the operating system, residin ...

10 Battery-powered distributed systems (extended abstract) 80%
Paul J. M. Havinga , Arne Helme , Sape J. Mullender , Gerard J. M. Smit , Jaap Smit
Proceedings of the 8th ACM SIGOPS European workshop on Support for composing distributed applications September 1998

11 Robust FPGA intellectual property protection through multiple small watermarks 80%
John Lach , William H. Mangione-Smith , Miodrag Potkonjak
Proceedings of the 36th ACM/IEEE conference on Design automation conference June 1999

12 Security issues for wireless ATM networks 77%
Danai Patiyoot
ACM SIGOPS Operating Systems Review January 2002
Volume 36 Issue 1
To be able to fulfil the need of user in wireless ATM, the system has to acquire features. One of the system features for the wireless ATM is functionality especially the security aspect. There is so far tittle, if not none, security consideration in the developing of wireless ATM standard. Therefore a wide range of features in security functions is in consideration. This paper tried to define the features of security in wireless ATM networks considering it features from existing fixed ATM netwo ...

13 Engineering a security kernel for Multics 77%
Michael D. Schroeder
Proceedings of the fifth symposium on Operating systems principles November 1975
This paper describes a research project to engineer a security kernel for Multics, a general-purpose, remotely accessed, multiuser computer system. The goals are to identify the minimum mechanism that must be correct to guarantee computer enforcement of desired constraints on information access, to simplify the structure of that minimum mechanism to make verification of correctness by auditing possible, and to demonstrate by test implementation that the security kernel so developed is capab ...

14 Tamper-resistant whole program partitioning 77%
Tao Zhang , Santosh Pande , Antonio Valverde
ACM SIGPLAN Notices , Proceedings of the 2003 ACM SIGPLAN conference on Language, compiler, and tool for embedded systems June 2003
Volume 38 Issue 7
Due to limited available memory (of the order of Kilobytes) on embedded devices (such as smart cards), we

undertake an approach of partitioning the whole program when it does not fit in the memory. The program partitions are downloaded from the server on demand into the embedded device just before execution. We devise a method of partitioning the code and data of the program such that no information regarding the control flow behavior of the program is leaked out. This property is called tamper ...

15 The information furnace: consolidated home control 77%

Diomidis D. Spinellis

Personal and Ubiquitous Computing May 2003

Volume 7 Issue 1

The Information Furnace is a basement-installed PC-type device that integrates existing consumer home-control, infotainment, security and communication technologies to transparently provide accessible and value-added services. A modern home contains a large number of sophisticated devices and technologies. Access to these devices is currently provided through a wide variety of disparate interfaces. As a result, end users face a bewildering array of confusing user-interfaces, access modes a ...

16 Code optimization II: Hiding program slices for software security 77%

Xiangyu Zhang , Rajiv Gupta

Given the high cost of producing software, development of technology for prevention of software piracy is important for the software industry. In this paper we present a novel approach for preventing the creation of unauthorized copies of software. Our approach splits software modules into *open* and *hidden* components. The open components are installed (executed) on an unsecure machine while the hidden components are installed (executed) on a secure machine. We assume that while open ...

17 Design analysis techniques: Energy-aware design techniques for differential power analysis protection 77%

Luca Benini , Alberto Macii , Enrico Macii , Elvira Omerbegovic , Fabrizio Pro , Massimo Poncino

Proceedings of the 40th conference on Design automation June 2003

Differential power analysis is a very effective cryptanalysis technique that extracts information on secret keys by monitoring instantaneous power consumption of cryptoprocessors. To protect against differential power analysis, power supply noise is added in cryptographic computations, at the price of an increase in power consumption. We present a novel technique, based on well-known power-reducing transformations coupled with randomized clock gating, that introduces a significant amount of scra ...

18 VLSI design: A novel architecture for power maskable arithmetic units 77%

L. Benini , A. Macii , E. Macii , E. Omerbegovic , M. Poncino , F. Pro

Proceedings of the 13th ACM Great Lakes Symposium on VLSI April 2003

Power maskable units have been proposed as a viable solution for preventing side-channel attacks to cryptoprocessors. This paper presents a novel architecture for the implementation of a class of such kinds of units, namely arithmetic components, which find wide usage in cryptographic applications and which are not suitable to traditional masking techniques. Results of extensive exploration and architectural trade-off analysis show the viability of the proposed solution.

19 On the parallel decomposability of geometric problems 77%

M. J. Atallah , J. J. Tsay

Proceedings of the fifth annual symposium on Computational geometry June 1989

There is a large and growing body of literature concerning the solution of geometric problems on mesh-connected arrays of processors [5,9,14,17]. Most of these algorithms are optimal (i.e., run in time &Ogr;(n1/d) on a d-dimensional n-processor array), and they all assume that the parallel machine is trying to solve a problem of size n on an n-processor array. What happ ...

20 Verifiable secret sharing and multiparty protocols with honest majority 77%

T. Rabin , M. Ben-Or

Proceedings of the twenty-first annual ACM symposium on Theory of computing February 1989

Under the assumption that each participant can broadcast a message to all other participants and that each pair of participants can communicate secretly, we present a verifiable secret sharing protocol, and show that any multiparty protocol, or game with incomplete information, can be achieved if a majority of the players are honest. The secrecy achieved is unconditional and does not rely on any assumption about computational intractability. Applications of these results to Byzantine Agreem ...